REMARKS

In the Official Action mailed on **21 December 2007**, the Examiner reviewed claims 4-12 and 16-18. Examiner rejected claims 7-9 under 35 U.S.C. § 112. Examiner rejected claims 4-12 and 16-18 under 35 U.S.C. § 101. Examiner rejected claims 4-12 and 16-18 under 35 U.S.C. § 102(b) based on Schneier ("Applied Cryptography" hereinafter "Schneier").

Rejections under 35 U.S.C. § 112

Examiner rejected claims 7-9 under 35 U.S.C. § 112 for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Accordingly, Applicant has amended claim 7 to delete the limitation "and the output of the first exclusive or operator." This amendment finds support in FIG. 7 and page 9, line 6 to page 10, line 14 of the instant application.

Rejections under 35 U.S.C. § 101

Examiner rejected claims 4-12 and 16-18 under 35 U.S.C. § 101. Applicant respectfully disagrees for at least the following reasons.

Applicant points out that the structure disclosed in claims 4, 7, 10, and 16 can be used to calculate a single round of the Data Encryption Standard technique. Accordingly, Applicant has amended claims 4, 7, 10, and 16 to clarify that these claims are directed to a structure that can perform **a given round of the Data Encryption Standard**. Furthermore, Applicant has amended claims 4, 7, 10, and 16 to clarify that the outputs of the exclusive-or operators for a given round of the Data Encryption Standard can be used for the next round of the Data

Encryption Standard. These amendments find support on page 6, line 9 to page 14, line 6 and FIGs. 5, 7, 8, and 12 of the instant application.

Applicant points out that the structures described in claims 4, 7, 10, and 16 satisfy the requirements of 35 U.S.C. § 101 because the structures produce a useful, concrete, and tangible result, and do not preempt a 35 U.S.C. § 101 judicial exception.

The claimed invention satisfies the *utility requirement* because it produces results that are *specific, substantial, and credible*. The claimed invention is *specific* because the claimed invention is specific to the claimed subject matter (i.e., an execution unit which is configured to calculate a given round of the Data Encryption Standard) and provides a well-defined and particular benefit to the public (e.g., faster calculations than a direct implementation of the Data Encryption Standard). The claimed invention is *substantial* because the results are useful to the public as disclosed in its current form. The claimed invention can be implemented in hardware and be used today to improve the speed of performing operations for the Data Encryption Standard. Furthermore, the claimed invention is *credible* because it is operative and produces results for a given round of the Data Encryption Standard.

The claimed invention satisfies the *tangible requirement* because the claimed invention is directed to hardware (i.e., a machine or apparatus) which implements a given round of the Data Encryption Standard.

The claimed invention satisfies the *concrete requirement* because the claimed invention produces repeatable results.

Furthermore, the claimed invention is a practical application of the Data Encryption Standard because it is one hardware implementation of the Data Encryption Standard. Hence, the claimed invention does not preempt a 35 U.S.C. § 101 judicial exception.

For these reasons, Applicant requests that the rejection based on 35 U.S.C. §101 be withdrawn.

Rejections under 35 U.S.C. § 102(b)

Examiner rejected claims 4-12 and 16-18 under 35 U.S.C. § 102(b) based on Schneier. Applicant respectfully disagrees for the following reasons. Note that as amended, the claims are directed to a given round of the Data Encryption Standard. Hence, the discussion below refers to a given round of the Data Encryption Standard.

Examiner avers that Schneier discloses "a first exclusive-or operator having two inputs and an output, the first exclusive-or operator configured to receive the Left Half input and the Key input" (see page 3 of the Office Action letter mailed on 21 December 2007). However, Schneier *does not disclose* an exclusive-or operator configured to receive **the Left Half input and the Key input**. At most, Schneier, discloses an exclusive-or operator which receives a **Left Half input and the output of a P-box permutation** (see Schneier pages 270, 275-277 "P-Box Permutation" and FIG. 12.2).

Moreover, Examiner avers that Schneier discloses "a second exclusive-or operator having two inputs and an output, the second exclusive-or operator configured to receive the data output by the first group of transistors (i.e., the S-box table lookups) and the output of the first exclusive-or operator" (see page 3 of the Office Action letter mailed on 21 December 2007). However, Schneier does not disclose an exclusive-or operator configured to receive **the data output by the first group of transistors and the output of the first exclusive-or operator**. Schneier discloses: (1) an exclusive-or operator which receives **an output from a compression permutation and an expansion permutation** (neither of which are outputs of an exclusive-or operator), and (2) an exclusive-or

operator which receives a **Left Half input and the output of a P-box permutation** (neither of which are outputs of an exclusive-or operator) (see Schneier FIG. 12.2).

Furthermore, Examiner avers that Schneier discloses "a third exclusive-or operator having two inputs and an output, the third exclusive-or operator configured to receive the Left Half input and the data output by the first group of transistors" (see page 3 of the Office Action letter mailed on 21 December 2007). However, Schneier does not disclose an exclusive-or operator configured to receive **the Left Half input and the data output by the first group of transistors** (i.e., the S-box table lookups). At most, Schneier discloses an exclusive-or operator which receives **the Left Half input and data from a P-box Permutation** (see Schneier FIG. 12.2 and page 274-277). Note that FIG. 12.2 of Schneier clearly indicates that the *S-box output is only used as the input to the P-box Permutation*.

Because Schneier does not disclose the structure as described in claims 4, 7, 10, and 16, Schneier does not anticipate these claims. Hence, Applicant respectfully submits that independent claims 4, 7, 10, and 16 as presently amended are in condition for allowance. Applicant also submits that claims 5-6, which depend upon claim 4, claims 8-9, which depend upon claim 7, claims 11-12, which depend upon claim 10, and claims 17-18, which depend upon claim 16, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Anthony Jones/
Anthony Jones
Registration No. 59,521

Date: 4 March 2007

Anthony Jones
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1666
Fax: (530) 759-1665
Email: tony@parklegal.com